(19)

Europäisches Patentamt

European Patent Office

Office européen des brevets

(11)   **EP 1 102 466 A2**

(12)   **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
23.05.2001 Bulletin 2001/21

(51) Int Cl.7: **H04N 1/00, H04N 1/32**

(21) Application number: 00310140.9

(22) Date of filing: 15.11.2000

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 15.11.1999 JP 32414799
31.01.2000 JP 2000022286

(71) Applicant: **CANON KABUSHIKI KAISHA**
Tokyo (JP)

(72) Inventor: **Suzuki, Takashi**
Ohta-ku, Tokyo (JP)

(74) Representative:
Beresford, Keith Denis Lewis et al
BERESFORD & Co.
High Holborn
2-5 Warwick Court
London WC1R 5DJ (GB)

(54)   **Information processing apparatus and processing method therefor**

(57)   In an image processing apparatus which has an operating system (102) and scanner driver (103), is connected to a scanner (104) for reading an original and converting it into an image signal, and stores image data read by manipulating the scanner (104), a forgery determination processing module (103-2) of the scanner driver (103) compares the read digital watermark data with specific image data to determine the matching degree, and an anti-forgery control module (106) controls predetermined image processing on the basis of the determination result for the image data read by the scanner driver (103).

FIG. 3
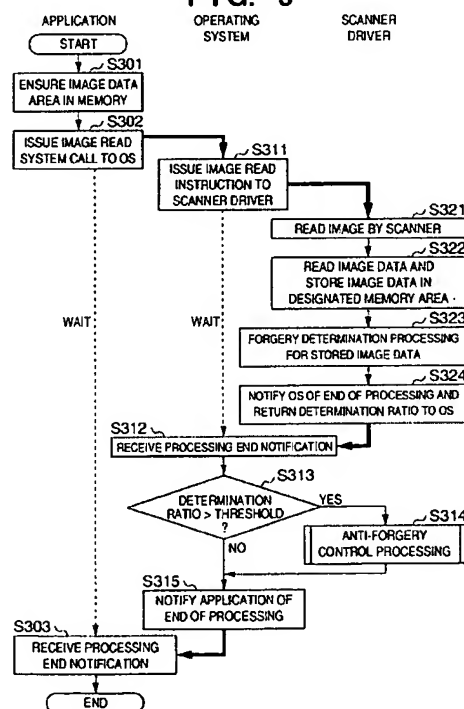
EP 1 102 466 A2

1   EP 1 102 466 A2   2

Description

FIELD OF THE INVENTION

[0001]   The present invention relates to an information processing apparatus in which an operating system can control read operation of an original image by a scanner via a scanner driver, or an information processing apparatus in which an operating system can control printing operation of image data by a printer via a printer driver, and a processing method therefor.

BACKGROUND OF THE INVENTION

[0002]   In recent years, color image reading apparatuses (to be referred to as color scanners hereinafter) using CCDs or the like as photoelectric conversion elements, and color printers have been improved in performance. This increases the risk of copying and forging copying-prohibited originals such as bank notes or securities by reading copying-prohibited originals such as bank notes or securities as image data by a color image reading apparatus and outputting them to a color printer. To prevent the forgery, a color copying machine as a combination of a color scanner and color printer often incorporates an anti-forgery apparatus which detects a copying-prohibited original to prohibit its copying.

[0003]   In addition, a so-called digital watermark technique of embedding information in an image so as not to recognize it with a naked eye is put into practice.

[0004]   However, an anti-forgery apparatus used in a color copying machine operates only in copying operation. If a copying-prohibited original is independently read once by a color scanner, the image of the copying-prohibited original can undesirably be output by the color copying machine or another color printer via a controller. Forgery processing by a system, e.g., scanner system or information processing apparatus capable of outputting image data to the color printer via a host computer cannot be effectively limited between the color scanner and the color printer. A serious problem of easily forging copying-prohibited originals arises.

[0005]   Furthermore, there is no information processing apparatus for outputting embedded information so as to easily recognize it.

[0006]   The present invention has been made to address one or more of the conventional drawbacks. An embodiment provides an information processing apparatus capable of allowing an operating system to control read operation of an original image by a scanner via a scanner driver, wherein image data read by the scanner driver is compared with specific image data to determine the matching degree, predetermined image processing for the image data read by the scanner driver is controlled on the basis of the determination result, and thus even in an environment in which the scanner is not constituted as a copying system integrated with a printer and can perform image read processing by the scanner

itself, when image data which matches a specific image whose copying operation is prohibited is read, the read illicit image data which matches the specific image is processed into insignificant image data, thereby reliably preventing image input processing of creating a forgery from a copying-prohibited original. An embodiment provides an information processing apparatus capable of allowing an operating system to control printing operation of image data by a printer via a printer driver, wherein image data rasterized by the printer driver is compared with specific image data to determine the matching degree, predetermined image processing for the image data rasterized by the printer driver is controlled on the basis of the determination result, and thus even in an environment in which the printer is not constituted as a copying system integrated with a scanner and can perform image output processing by the printer itself, when image data which matches a specific image whose copying operation is prohibited is rasterized, the rasterized illicit image data which matches the specific image is processed into insignificant image data, thereby reliably preventing image output processing of creating a forgery from a copying-prohibited original. Embodiments also provide processing methods therefor.

[0007]   A further object is to provide an information processing apparatus capable of extracting information embedded in an image, processing the extracted information into an image, and outputting the image, and a processing method therefor.

[0008]   In an embodiment, an information processing apparatus capable of controlling read operation of an original image by a scanner (scanner 104 shown in Fig. 2) via a scanner driver (corresponding to a scanner driver 103 shown in Fig. 2) comprises determination means (corresponding to a forgery determination processing module 103-2 shown in Fig. 2) for determining by the scanner driver whether digital watermark information is embedded in image data read by the scanner, and control means (corresponding to an anti-forgery control module 106 shown in Fig. 2) for controlling predetermined image processing for the read data on the basis of a determination result by the determination means.

[0009]   The control means may process the read image data into image data different from the read image data when the determination means determines that the image data substantially matches the specific image data.

[0010]   Display means (monitor 109 shown in Fig. 2) may be provided for displaying a warning message representing that the image data is processed to match the specific image data when the control means performs the predetermined image processing for the image data, and the control means may discard the read and processed image data on the basis of an image processing request from a user in response to the warning message displayed on the display means.

[0011]   The predetermined image processing may include resolution conversion processing of converting a

resolution of the read image data, color conversion processing of converting color tone of the read image data, and image conversion processing of adding arbitrary image data to the read image data.

[0012] The control means may create log information from which a read processing status of the specific image data can be verified, and may register the log information in a nonvolatile memory on the basis of the image processing request from the user in response to the warning message displayed on the display means.

[0013] The specific image data may include an original image whose copying operation is prohibited by law.

[0014] The specific image data may be stored and managed in advance so as to be updateable.

[0015] The scanner can be connected via a local interface or a network interface.

[0016] The digital watermark information may be embedded in the specific image data at a predetermined cycle.

[0017] The digital watermark information may include, as code information, information about the type of specific image data, an issue country, an issue number, and a value.

[0018] The digital watermark information may include invisible or visible information.

[0019] Storage means may be provided for storing image data read by the scanner, and the control means may also process an image stored in the storage means.

[0020] In an embodiment, an image processing method for an information processing apparatus capable of controlling read operation of an original image by a scanner (scanner 104 shown in Fig. 2) via a scanner driver (corresponding to the scanner driver 103 shown in Fig. 2) comprises the determination step of determining by the scanner driver whether digital watermark information is embedded in image data read by the scanner, and the control step of controlling predetermined image processing for the read image data on the basis of a determination result in the determination step.

[0021] The control step (step S601 shown in Fig. 8) may comprise processing the read image data into image data different from the read image data when the image data is determined in the determination step to substantially match the specific image data.

[0022] A display step (step S602 shown in Fig. 8) may be provided of displaying a warning message representing that the image data is processed to match the specific image data when the predetermined image processing is performed for the image data in the control step, and the control step may comprise discarding (step S604 shown in Fig. 8) the read and processed image data on the basis of an image processing request from a user in response to the warning message displayed in the display step.   •

[0023] The predetermined image processing may include resolution conversion processing of converting a resolution of the read image data, color conversion processing of converting color tone of the read image

data, and image conversion processing of adding arbitrary image data to the read image data.

[0024] The control step may comprise creating log information from which a read processing status of the specific image data can be verified, and registering the log information in a nonvolatile memory (corresponding to a hard disk 108 shown in Fig. 2) on the basis of the image processing request from the user in response to the warning message displayed in the display step.

[0025] An embodiment of the invention also provides a recording medium storing in a computer-readable manner a program for causing an information processing apparatus capable of controlling read operation of an original image by a scanner (scanner 104 shown in Fig. 2) via a scanner driver (corresponding to the scanner driver 103 shown in Fig. 2), to execute the determination step of determining by the scanner driver whether digital watermark information is embedded in image data read by the scanner, and the control step of controlling predetermined image processing for the read image data on the basis of a determination result in the determination step.

[0026] The program may define the control step (step S601 shown in Fig. 8) to comprise processing the read image data into image data different from the read image data when the image data is determined in the determination step to substantially match the specific image data.

[0027] The program may include a program for causing the information processing apparatus to execute the display step (step S602 shown in Fig. 8) of displaying a warning message representing that the image data is processed to match the specific image data when the predetermined image processing is performed for the image data in the control step, and the control step comprises discarding (step S604 shown in Fig. 8) the read and processed image data on the basis of an image processing request from a user in response to the warning message displayed in the display step.

[0028] The program may define the predetermined image processing to include resolution conversion processing of converting a resolution of the read image data, color conversion processing of converting color tone of the read image data, and image conversion processing of adding arbitrary image data to the read image data.

[0029] The program may define the control step to comprise creating log information from which a read processing status of the specific image data can be verified, and registering the log information in a nonvolatile memory (corresponding to the hard disk 108 shown in Fig. 2) on the basis of the image processing request from the user with respect to the warning message displayed in the display step.

[0030] An embodiment of the invention also provides an information processing apparatus capable of controlling read operation of an original image by a scanner (scanner 104 shown in Fig. 15) via a scanner driver (cor-

5   EP 1 102 466 A2   6

responding to the scanner driver 103 shown in Fig. 15) comprising information extraction means (corresponding to a digital watermark extraction module 103-3 shown in Fig. 15) for extracting, by the scanner driver, digital watermark information embedded in image data read by the scanner, and image processing means (corresponding to an image processing control module 116 shown in Fig. 15) for processing the image data on the basis of an extraction result from said information extraction means.

[0031] Selection means (corresponding to a monitor 109 shown in Fig. 15) may also be provided for causing a user to select whether to process the image data by the image processing means.

[0032] The selection means may display whether to process the image data on display means, thereby causing the user to select whether to process the image data.

[0033] The image processing means may overlay the information extracted by the information extraction means on the image data.

[0034] An embodiment of the invention also provides a processing method for an information processing apparatus capable of controlling read operation of an original image by a scanner via a scanner driver comprises an information extraction step (step S423 shown in Fig. 16) of extracting, by the scanner driver, digital watermark information embedded in image data read by the scanner, and an image processing step (step S413 shown in Fig. 16) of processing the image data on the basis of an extraction result in the information extraction step.

[0035] An embodiment of the invention also provides a recording medium storing in a computer-readable manner a program for causing an information processing apparatus capable of controlling read operation of an original image by a scanner via a scanner driver, to execute an information extraction step of extracting, by the scanner driver, digital watermark information embedded in image data read by the scanner, and an image processing step of processing the input image data on the basis of an extraction result.

[0036] Other features and advantages of embodiments will be apparent from the following description taken in conjunction with the accompanying drawings, in which like reference characters designate the same or similar parts throughout the figures thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

[0037]

Fig. 1 is a block diagram showing an example of an image processing system to which an information processing apparatus according to the first embodiment of the present invention can be applied;
Fig. 2 is a block diagram for explaining the internal structure of the OS in the host computer 21 shown

in Fig. 1;
Fig. 3 is a flow chart showing an example of the first data processing sequence in the information processing apparatus according to the present invention;
Figs. 4A and 4B are views showing an example of anti-forgery processing by an operating system shown in Fig. 2;
Fig. 5 is a graph showing an example of image data processing by the operating system shown in Fig. 2;
Fig. 6 is a view showing an example of a user interface window displayed on a monitor shown in Fig. 2;
Fig. 7 is a view showing an example of log information stored in a hard disk shown in Fig. 2;
Fig. 8 is a flow chart showing an example of the second data processing sequence in the information processing apparatus according to the present invention;
Fig. 9 is a block diagram showing an example of an information processing apparatus according to the second embodiment of the present invention;
Fig. 10 is a graph showing an image processing principle for image data to be forged in the information processing apparatus according to the present invention;
Fig. 11 is a view showing an example of image processing in an information processing apparatus according to the third embodiment of the present invention;
Fig. 12 is a view showing another example of image processing in the information processing apparatus according to the third embodiment of the present invention;
Fig. 13 is a view showing still another example of image processing in the information processing apparatus according to the third embodiment of the present invention;
Fig. 14 is a view for explaining the memory map of a storage medium which stores various data processing programs readable by the information processing apparatus according to the present invention;
Fig. 15 is a block diagram showing the arrangement of an image processing system in the fourth embodiment;
Fig. 16 is a flow chart showing the processing sequence of the system in the fourth embodiment;
Fig. 17 is a view showing an example of a user interface window displayed on a monitor 109;
Figs. 18A and 18B are views showing an example of image processing according to the fourth embodiment;
Fig. 19 is a view showing an example of log information stored in a hard disk 108;
Fig. 20 is a block diagram showing the arrangement of an image processing system in the fifth embodiment;
Fig. 21 is a flow chart showing the processing se-

quence of the system in the fifth embodiment; and Fig. 22 is a view for explaining the memory map of a storage medium which stores various data processing programs readable by the information processing apparatus according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[First Embodiment]

[0038] Fig. 1 is a block diagram showing an example of an image processing system to which an information processing apparatus according to the first embodiment of the present invention can be applied. As shown in Fig. 1, this system is built by a printer 23 and scanner 22, including a host computer (information processing apparatus) 21. This system may be built as a scanner system by the host computer 21 and scanner 22, or as a printer system by the host computer 21 and printer 23. Alternatively, the system may be built by only either of the systems. The system may use a plurality of scanners or printers. The present invention can be applied to any connection form regardless of a network or local connection.

[0039] An operating system (to be referred to as an "OS" hereinafter) 102 shown in Fig. 2 runs on the host computer 21. A scanner manipulation application (application) 101 running on the OS provides a manipulation environment for, e.g., image read operation of a scanner 104 (corresponding to the scanner 22 shown in Fig. 1).

[0040] In Fig. 1, the host computer 21 as a scanner system comprises a monitor 201 for displaying the GUI of the application 101 or an image read result from the scanner 22, a mouse 202 for transferring a user input to the application and OS, a keyboard 203, an HDD 208 for storing various programs and image data, a ROM 206 for storing the basic programs of the host computer 21, a RAM 205 for reading a program and storing an image, and a scanner I/F 207 for controlling the scanner 22. The monitor 201, mouse 202, keyboard 203, HDD 208, ROM 206, RAM 205, and scanner I/F 207 are connected to each other via an internal bus 209, and controlled by a CPU 204.

[0041] The host computer 21 as a printer system comprises the monitor 201 for displaying the GUI of an application 701 (to be described later) shown in Fig. 9 or an image to be output to the printer 23, the mouse 202 for transferring a user input to the application and OS, the keyboard 203, the HDD 208 for storing various programs and image data, the ROM 206 for storing the basic programs of the host computer 21, the RAM 205 for loading a program and storing an image, and a printer I/F 210 for controlling the printer 23. The monitor 201, mouse 202, keyboard 203, HDD 208, ROM 206, RAM 205, and printer I/F 210 are connected to each other via the internal bus 209, and controlled by the CPU 204.

[0042] Both the OS and application are realized on the host computer 21 having this arrangement by running by the CPU 204 a program loaded from the HDD 208 to the RAM 205.

[0043] The internal structure of the OS will be explained within a range necessary for this system.

[0044] Fig. 2 is a block diagram for explaining the internal structure of the OS in the host computer 21 shown in Fig. 1. Note that most of OSs such as UNIX isolatedly mount a device driver which interfaces with hardware such as a scanner, and various modules for performing management of other user applications, memory management, and the like. In this embodiment, an OS having this isolation structure will be exemplified. In Fig. 2, the OS 102 has a scanner driver 103 as a module for controlling a user input and another hardware device, and in addition controlling the scanner 104. The scanner driver 103 in the first embodiment comprises a scanner control module 103-1 for directly controlling the scanner 104 and a forgery determination processing module 103-2 for determining whether an image received from the scanner 104 is an copying-prohibited original.

[0045] The OS 102 has a memory management module 105 for managing the image data area of an image memory 110 which stores image data received from the scanner 104. The image memory 110 is part of the RAM 205 shown in Fig. 1.

[0046] The application 101 is made up of a GUI routine for interfacing with the user, a routine for interpreting a user input received via the OS 102 and issuing an instruction for operating the scanner 104, a routine for displaying image data read from the scanner 104, and a routine for saving read image data in an HDD 108.

[0047] The scanner 104 scans an original placed on a table with a CCD line sensor (not shown) in accordance with a scanner manipulation signal from the scanner driver 103 to optically read the original, converts the image data into an electrical signal (photoelectric conversion), and returns the image signal to the host computer 21 (more specifically, the scanner control module 103-1 of the scanner driver 103) in accordance with a predetermined interface rule.

[0048] The image signal is comprised of a plurality of color components, e.g., R, G, and B, and each color component is multilevel data of 8 to 12 bits.

[0049] The data processing sequence of the scanner system shown in Fig. 2 will be explained on the basis of a flow chart shown in Fig. 3.

[0050] Fig. 3 is a flow chart showing an example of the first data processing sequence in the information processing apparatus according to the present invention. This data processing sequence corresponds to a data processing sequence between the modules of the application 101, OS 102, and scanner driver 103 shown in Fig. 2. S301 to S303 shown in Fig. 3 correspond to the steps of the application 101; S311 to S315, to the steps of the operating system 102; and S321 to S324,

to the steps of the scanner driver 103.

[0051]   When the user instructs scanning start operation via the GUI of the application 101, the application 101 advances to step S301. Before read operation starts, the application 101 ensures in the image memory 110 (RAM 205) the area of an image to be read that is designated by the user. Note that the image area on the image memory 110 is ensured by the memory management module 105. In step S302, the application 101 specifies the scanner 104 to be used to the OS 102, issues an image read instruction, and enters a wait state and stays there until the application 101 receives an image read processing end notification in step S303.

[0052]   The OS 102 which has received the scanning start instruction shifts to step S311, and invokes the scanner driver 103 corresponding to the specified scanner (in the first embodiment, the local-connected scanner 104) to issue an image read instruction to the scanner driver 103. The OS 102 enters a wait state and stays there until the OS 102 receives a processing end notification from the scanner driver 103 in step S312. At this time, the OS 102 prepares as a variable a determination ratio representing whether image data is a copying-prohibited original so that the forgery determination processing module 103-2 determines the determination ratio.

[0053]   The scanner control module 103-1 in the scanner driver 103 that has received the image read start instruction from the OS 102 advances to step S321, and issues a scanning start instruction unique to the scanner to the scanner 104 to start image read by the scanner 104. In step S322, the scanner control module 103-1 receives an image signal of an original image read by the scanner 104, stores the image signal in the image area in the image memory 110 (RAM 205) ensured by the application 101, and shifts processing to the forgery determination processing module 103-2 in the scanner driver 103.

[0054]   Note that the forgery determination processing module 103-2 has a copying-prohibited pattern as a template in a memory (RAM or ROM) arranged separately from the image memory 110.

[0055]   In step S323, the forgery determination processing module 103-2 executes pattern matching between the template and the image data stored in the image memory 110 (RAM 205), and outputs the matching result as a determination ratio having a value from "0" to "100". As an example of this pattern matching, the correlation between the image data and the template is calculated for each color component to output a maximum value. However, the pattern matching method in the first embodiment is not particularly limited.

[0056]   A plurality of copying-prohibited pattern templates may be prepared. In this case, the forgery determination processing module 103-2 performs pattern matching between a plurality of patterns and image data, and outputs a maximum value.

[0057]   The first embodiment has described the for-

gery determination processing module 103-2 as a software module. However, the forgery determination processing module 103-2 is not limited to this, and can be realized as hardware processing constituted by, e.g., a high-speed RISC and ASIC to increase the speed.

[0058]   After the image data is read and subjected to forgery determination processing, the scanner driver 103 notifies in step S324 the OS 102 of the end of read processing, and at the same time returns the determination ratio as a result of pattern matching with the copying-prohibited pattern.

[0059]   If the OS 102 receives the processing end notification from the scanner driver 103 in step S312, the OS 102 shifts to step S313, and checks whether the image data is a copying-prohibited image, on the basis of the result (determination ratio) of actually performing forgery determination processing by the forgery determination processing module 103-2. If the determination ratio is higher than a threshold set in advance on the OS 102 side, the OS 102 determines that the image data read by the scanner 104 may be a copying-prohibited image at a high possibility. Then, the OS 102 advances to step S314 to perform anti-forgery control processing (to be described in later).

[0060]   If the determination ratio is determined in step S313 to be lower than the pre-set threshold, or anti-forgery control processing ends, the OS 102 shifts to step S315, and issues a processing end notification to the application 101 to end image read operation of the scanner system.

[0061]   Figs. 4A and 4B are views showing an example of anti-forgery processing by the operating system 102 shown in Fig. 2, and corresponds to an anti-forgery processing state to a bank note whose copying operation is prohibited. Fig. 4A represents an original image read by the scanner 104, and Fig. 4B represents a processed image.

[0062]   Fig. 5 is a graph showing an example of image data processing by the operating system 102 shown in Fig. 2. The ordinate represents image data (Green), and the abscissa represents the scanning position. I in Fig. 5 indicates original image data, and II indicates processed image data.

[0063]   Fig. 5 shows Green data at part of an image along the ordinate, and the main scanning position of the image along the abscissa. The ordinate represents that image data has 256 gray levels from "0" to "255". As image data is nearer "255", the image is bright. Image data I means original image data before processing. By setting image data to a smaller value by a given value for all the pixels of the image data, image data II is generated. Of image data II, all data of "0" or less are "0", so that tonal information of the image is lost. This processing is executed for Red and Blue except Green to generate image Fig. 4B as an output image candidate.

[0064]   The first embodiment cannot return a processed image to an image before processing. From this,

11   EP 1 102 466 A2   12

an image displayed on a monitor 109 by the application 101 and an image saved in an HDD 108 are all processed images.

[0065] Fig. 6 is a view showing an example of a user interface window displayed on the monitor 109 shown in Fig. 2, and corresponds to a warning window example displayed to the user when image data read by the scanner 104 is detected as copying-prohibited image data. In Fig. 6, BT1 is a button which is selected and clicked by the user when the user approves the contents of a displayed warning and outputs an image. BT2 is a button which is selected and clicked by the user when the user approves the contents of a displayed warning and avoids outputting an image.

[0066] Fig. 7 is a view showing an example of log information stored in the hard disk 108 shown in Fig. 2. This log information corresponds to a manipulation log of the scanner 104. In Fig. 7, the manipulation log includes the time, host computer information (manufacturer name, host ID, and OS version), image size, and determination ratio.

[0067] Anti-forgery control processing (S314) shown in Fig. 3 will be described in detail with reference to a flow chart shown in Fig. 8.

[0068] Fig. 8 is a flow chart showing an example of the second data processing sequence in the information processing apparatus according to the present invention, and corresponds to the anti-forgery control processing sequence in step S314 shown in Fig. 3. Note that reference symbols S600 to S605 denote steps.

[0069] Processing starts in step S600, and an image in the image memory 110 undergoes anti-forgery image processing in step S601.

[0070] In the first embodiment, original image Fig. 4A undergoes processing to generate an image painted out with gray as processed image Fig. 4B. More specifically, as shown in Fig. 5, the processing principle is to perform image processing for original image data I and generate image data II.

[0071] Assuming that image data I is comprised of R (Red), G (Green), and B (Blue) color signals, the user input window shown in Fig. 6 is displayed on the monitor 109 via a display driver 107. Accordingly, when an image input by the scanner 104 may be a copying-prohibited original, the user is made to confirm whether to actually read the image.

[0072] In step S603, it is checked whether either of the buttons on the user input window, i.e., "OK". corresponding to the button BT1 and "Cancel" corresponding to the button BT2 has been selected and clicked. If "OK" has been selected and clicked (if the image is to be read), a manipulation log as shown in Fig. 7 is stored in the HDD 108, and processing ends in step S605. The operation that the copying-prohibited original has been read can be left as an evidence, which facilitates confirming whether the copying-prohibited original has been input.

[0073] If "Cancel" is determined in step S603 to be selected and clicked, that is, the image is not to be read, the image memory 110 storing the image is freed, no image read is performed, and processing ends in step S605.

[0074] As described above, according to the first embodiment, the information processing apparatus, which can control read operation of an original image by the scanner via the scanner driver by the operating system, compares image data read by the scanner driver with specific image data to determine the matching degree, controls predetermined image processing for the image data read by the scanner driver on the basis of the determination result, and thus even in an environment which can perform image read processing by the scanner itself (not use a printer), when image data which matches a specific image whose copying operation is prohibited is read, processes the read illicit image data which matches the specific image into insignificant image data, thereby reliably preventing image input processing of creating a forgery from a copying-prohibited original.

[Second Embodiment]

[0075] The first embodiment has described a case wherein predetermined image processing is executed in a scanner system for an input image of an anti-forgery target original. The present invention is not limited to this, and anti-forgery processing can be done in, e.g., a printer system as well. This embodiment will be explained.

[0076] Fig. 9 is a block diagram showing an example of an information processing apparatus according to the second embodiment of the present invention. According to the second embodiment, anti-forgery processing is performed by a printer driver 703 and OS 702 shown in Fig. 9 in an image processing system built by a host computer 21 and printer 23 shown in Fig. 1. Similar to the first embodiment, the OS 702 runs on the host computer 21, and an application 701 running on the OS 702 provides a manipulation environment for image output operation to a printer 704 (corresponding to the printer 23 shown in Fig. 1).

[0077] Similar to the scanner system shown in Fig. 2, the printer system shown in Fig. 9 is also implemented on a hardware arrangement shown in Fig. 1. This system is built by the host computer 21 and printer 23 (printer 704 in Fig. 9). Both the OS and application on the host computer 21 realize anti-forgery processing in the printer system by running by a CPU 204 a program loaded from an HDD 208 to a RAM 205. In Fig. 9, the OS 702 has a printer driver 703 as a module for controlling a user input and another hardware device, and in addition controlling the printer. The printer driver 703 comprises a rasterizer 703-1 for generating image data suitable for the printer 704, a memory management module 703-2 for managing an image memory 710 for storing the generated image data, and a forgery determination

processing module 703-3 for determining whether the rasterized image is a copying-prohibited original.

[0078]   A forgery determination result output from the forgery determination processing module 703-3 is transferred to an anti-forgery control module 705 which performs processing for preventing or suppressing forgery operation on the basis of the determination result.

[0079]   The OS 702 has a printing spooler 709 for performing control for outputting an image rasterized by the rasterizer 703-1 in the printer driver 703 to the printer 704. In this embodiment, the rasterizer 703-1 and forgery determination processing module 703-3 are operated by the printer driver 703, i.e., by software processing, but can be operated on the printer 704 side.

[0080]   In this case, the result of forgery determination processing performed on the printer 704 side is returned to the anti-forgery control module 705. The flow of anti-forgery processing in the second embodiment will be explained.

[0081]   When the OS 702 which has received a printing instruction command via the GUI of the application 701 requests of the printer driver 703 printing processing of data received from the application 701, the printer driver 703 which has received the printing processing request uses the rasterizer 703-1 to rasterize a printing document as image data, and stores the image data in the image memory 710. The image data stored in this manner is transferred to the forgery determination processing module 703-3 and printing spooler 709 which start forgery determination processing and printing processing, respectively.

[0082]   Similar to the first embodiment, the forgery determination processing module 703-3 determines by pattern matching whether an image to be printed contains a copying-prohibited pattern, and outputs the result as a determination ratio to the anti-forgery control module 705.

[0083]   The anti-forgery control module 705 compares a threshold set in advance in the OS 702 with the determination ratio as an output value from the forgery determination processing module 703-3. When the determination ratio is higher, anti-forgery control module 705 executes image processing similar to Figs. 4A and 4B, and displays a warning dialogue similar to the one shown in Fig. 6 on a monitor 708.

[0084]   Fig. 10 is a graph for explaining the image processing principle of the printer system for image data to be forged. In Fig. 10, the ordinate represents Yellow data at part of an image, and the abscissa represents the main scanning position of the image. For example, when image data is in a color space format of M (Magenta), C (Cyan), Y (Yellow), and BK (BlacK), the image data has 256 tone levels from "0" to "255". As image data is nearer "255", the image is dark.

[0085]   In Fig. 10, image data I means original image data before processing. By setting image data to a larger value by a given value for all the pixels of the image data, processed image data II is generated. Of image data II, all data of "255" or more are "255", so that tonal information of the image is lost. This processing is executed for Magenta, Cyan, and Black as well as Yellow to output image in Fig. 4B.

[0086]   Similar to the first embodiment, the second embodiment cannot return a processed image to an image before processing. From this, an image displayed on the monitor 708 from the application 701 or an image saved in an HDD 706 is also a processed image.

[0087]   When the user determines not to perform printing on the dialogue shown in Fig. 6 (when the button BT2 is selected and clicked), a spool stop instruction is issued to the spooler 709, and printing processing ends.

[0088]   To the contrary, when the user determines to perform printing on the dialogue shown in Fig. 6 (when the button BT1 is selected and clicked), manipulation log information shown in Fig. 7 is stored in the hard disk 706 to end printing processing. As a result, when image data to be printed is similar to anti-forgery target image data, the image to be printed is printed out as a processed image, and image data II shown in Fig. 10 is not output directly, i.e., as an original image.

[0089]   As described above, according to the second embodiment, the information processing apparatus in which the operating system can control printing operation of image data by the printer via the printer driver compares image data rasterized by the printer driver with specific image data to determine the matching degree, controls predetermined image processing for the image data rasterized by the printer driver on the basis of the determination result, and thus even in an environment which can perform image output processing by the printer itself (not use a scanner), when image data which matches a specific image whose copying operation is prohibited is rasterized, processes the rasterized illicit image data which matches the specific image into insignificant image data, thereby reliably preventing image output processing of creating a forgery from a copying-prohibited original.

[Third Embodiment]

[0090]   The first and second embodiments have described a case wherein the tint component of image data is processed into a tint component different from an original. However, anti-forgery image processing of the present invention is not limited to this, and may be modified to perform processing of thinning input image data to decrease the resolution, decreasing the gray levels of image data, or replacing image data stored in image data or generated with another image data and rasterizing the replaced image data.

[0091]   Alternatively, processing of leaving only one color of R, G, and B, or M, C, Y, and BK and erasing images of the remaining colors may be executed. These processes may be appropriately combined. This embodiment will be explained.

[0092]   Figs. 11, 12, and 13 are views each showing

an example of image processing in an image processing system according to the third embodiment of the present invention. In Fig. 11, part of an original image 11-1 is enlarged and represented in units of pixels to obtain an enlarged main part image 11-2. If pixels to be left in target image data 12-1 corresponding to the enlarged main part image 11-2 shown in Fig. 11 are designated with arrows, image processing of extracting only information of the pixels designated by the arrows is executed to generate image data 12-2 to be output. In the example shown in Fig. 12, the resolution is decreased by simply thinning information every other pixel. After the resolution is decreased, the image data is output as one reduced to 1/2 (50%) the image data before the resolution is decreased.

[0093] When image data before processing is made up of color signals of R (Red), G (Green), and B (Blue), and image data of each color signal is 8-bit data representing 256 gray levels from "0" to "255", the resolution is decreased by fixing lower 4 bits to 0 without changing upper 4 bits.

[0094] Fig. 13 is an image as a result of performing anti-forgery image processing for original data shown in Fig. 4A when another image is to be added to image data.

[0095] In the example shown in Fig. 13, image data of pixels corresponding to characters "COPY" are added to an original image. Note that only one color of R, G, and B, or M, C, Y, and BK may be left, and images of the remaining colors may be erased.

[0096] In this case, for, e.g., R, G, and B, image data of Red as one separated color is left without any processing, and data of all the pixels are changed to "255" for image data of the remaining Green and Blue colors.

[0097] According to the first to third embodiments, forgery operation can be suppressed by the scanner driver or printer driver, and thus the forgery suppression effect can be expected for all image inputs from scanners and image outputs to printers.

[0098] The configuration of a data processing program readable by the information processing apparatus according to the present invention will be explained with reference to a memory map shown in Fig. 14.

[0099] Fig. 14 is a view for explaining the memory map of a storage medium which stores various data processing programs readable by the information processing apparatus according to the present invention.

[0100] Although not shown, this storage medium sometimes stores information for managing programs stored in the storage medium, such as version information and programmer name, and information depending on the OS of the program reading side, such as an icon for discriminatively displaying a program.

[0101] Further, data subordinate to various programs are also managed by directory information. In some cases, the storage medium also stores a program for install-

ing various programs in a computer, or a program for decompressing a program to be installed when the program is compressed.

[0102] The functions shown in Figs. 3 and 8 may be achieved by the host computer 21 in accordance with an externally installed program. The present invention is also applied to a case wherein pieces of information including a program are supplied to an output apparatus from a storage medium such as a CD-ROM, flash memory, or FD, or from an external storage medium via a network.

[0103] In the first to third embodiments, the anti-forgery control module saves a copying-prohibited pattern as a template for image data (scanner driver) input by the scanner or rasterized image data (printer driver), and performs pattern matching to determine whether the image data matches a copying-prohibited image. This determination is not limited to pattern matching. When digital watermark information representing a copying-prohibited image is embedded in the copying-prohibited image, this digital watermark may be held by the anti-forgery control module, and detected from the (input or rasterized) image data to determine the presence of the copying-prohibited image.

[0104] Note that the digital watermark may be one which is embedded in a specific frequency in an image and cannot be recognized with a naked eye, or one which is embedded in a copying-prohibited image with an unnoticeable size and color and can be visually recognized. The digital watermark is preferably embedded in the pattern of a copying-prohibited image because the digital watermark cannot be visually recognized.

[0105] The digital watermark may contain, as code information, information about the type of copying-prohibited image, the issue country, the issue number, and the value. This information may be determined by the forgery determination module, and stored as log information as shown in Fig. 7. If the log information is stored in the folder of the HDD 108 by encrypting this information so as not to decrypt it without using a dedicated application, the log of processing the copying-prohibited image can be stored with high security.

[0106] When the copying-prohibited image is processed by the anti-forgery control module, the log information shown in Fig. 7 may be added as a digital watermark to a processed image. With this processing, even if an image is formed using a printer driver having no forgery determination module, the added digital watermark can be detected from the print by the scanner driver.

[Fourth Embodiment]

[0107] A case wherein an information processing apparatus reads an original by a scanner, and if information (digital watermark) which cannot be recognized with a naked eye is embedded in the read original, executes predetermined image processing will be explained as

the fourth embodiment of the present invention.

[0108] The arrangements of an information processing apparatus, scanner, and printer in the fourth embodiment are the same as those shown in Fig. 1, and a description thereof will be omitted.

[0109] Fig. 15 is a block diagram showing the arrangement of an image processing system in the fourth embodiment, and shows in detail the internal structure of the operating system (OS) of a host computer 21. Note that most of OSs such as UNIX isolatedly mount a device driver which interfaces with hardware such as a scanner, and various modules for performing management of other user applications, memory management, and the like. In this embodiment, an OS having this isolation structure will be exemplified.

[0110] As shown in Fig. 15, an OS 102 has a scanner driver 103 as a module for controlling a user input and another hardware device, and in addition controlling a scanner 104. The scanner driver 103 in the fourth embodiment comprises a scanner control module 103-1 for directly controlling the scanner 104 and a digital watermark extraction module 103-3 for extracting information (digital watermark) embedded in image data from the image data read by the scanner 104.

[0111] The OS 102 comprises an image processing control module 116 for executing image processing control processing (to be described in detail later) in accordance with the extraction result from the digital watermark extraction module 103-3, and a display driver 107 for displaying image data read by the scanner 104, a user interface window, or the like on a monitor 109.

[0112] Further, the OS 102 comprises a memory management module 105 for managing an image data area as an image memory 110 (part of a RAM 205)

[0113] A scanner manipulation application (application) 101 is made up of a GUI routine for interfacing with the user, a routine for interpreting a user input received via the OS 102 and issuing an instruction for operating the scanner 104, a routine for displaying image data read from the scanner 104, and a routine for saving read image data in an HDD 108.

[0114] The scanner 104 sends, to the host computer 21 in accordance with a predetermined interface rule, image data obtained by scanning an original placed on a table with a CCD line sensor (not shown) in accordance with a scanner manipulation command (signal) from the scanner driver 103, optically reading the original, and converting the image data into an electrical signal (photoelectric conversion).

[0115] The image signal is comprised of luminance signals of color components, e.g., R, G, and B, and each luminance signal is multilevel data of 8 to 12 bits.

[0116] An operation of reading an original by the scanner 104, and if information (digital watermark) which cannot be recognized with a naked eye is embedded in the read original, executing predetermined image processing will be explained.

[0117] Fig. 16 is a flow chart showing an example of the processing sequence of the system in the fourth embodiment. This processing corresponds to data processing between the modules of the application 101, OS 102, and scanner driver 103 shown in Fig. 15. S401 to S403 shown in Fig. 16 correspond to the steps of the application 101; S411 to S415, to the steps of the operating system 102; and S421 to S424, to the steps of the scanner driver 103.

[0118] When the user instructs scanning start operation via the GUI of the application 101, the application 101 advances to step S401. Before read operation starts, the application 101 ensures in the image memory 110 (RAM 205) the area of an image to be read that is designated by the user. Note that the image area on the image memory 110 is ensured by the memory management module 105. In step S402, the application 101 specifies the scanner 104 to the OS 102, issues an image read instruction, and enters a wait state and stays there until the application 101 receives an image read processing end notification in step S403.

[0119] In step S411, the OS 102 which has received the scanning start instruction invokes the scanner control module 103-1 of the scanner driver 103 corresponding to the specified scanner (in the fourth embodiment, the scanner 104) to issue an image read instruction with the scanner 104. The OS 102 enters a wait state and stays there until processing of the scanner driver 103 ends. At this time, the OS 102 prepares a variable for information extracted from a digital watermark in image data output from the digital watermark extraction module 103-3.

[0120] In step S421, the scanner control module 103-1 in the scanner driver 103 that has received the scanning start instruction from the OS 102 issues a scanning start instruction unique to the scanner to the scanner 104 to read an image. In step S422, after image data of the original is read, the scanner control module 103-1 stores image data received from the scanner 104 in the ensured image data area of the application 101 in the image memory 110 (RAM 205), and shifts processing to the digital watermark extraction module 103-3.

[0121] Digital watermark extraction processing in the digital watermark extraction module 103-3 will be explained.

[0122] The digital watermark extraction module 103-3 divides the input image data into blocks, and performs Fourier transformation for each block to extract a frequency component. The digital watermark extraction module 103-3 separates image data of the obtained frequency area into an amplitude spectrum and phase spectrum, and detects a registration signal contained in the amplitude spectrum.

[0123] The registration signal is embedded by an impulse signal to a frequency of an intermediate level which is equal to or lower than the first frequency level at which the registration signal is hardly recognized by the human perception, and equal to or higher than the

second frequency at which the registration signal is not removed by irreversible compression/decompression, in consideration of the drawbacks of a high-frequency component and low-frequency component that embedding of a signal in a low-frequency component is readily recognized as noise by the visual characteristic of the human, as compared to embedding of a signal in a high-frequency component, and that an irreversible compression method such as JPEG compression has a low-pass filter effect and the high-frequency component is removed by compression/decompression processing.

[0124]   In registration detection, the digital watermark extraction module 103-3 extracts the impulse signal in the intermediate-level frequency range included in the amplitude spectrum. The digital watermark extraction module 103-3 calculates the scaling factor of digital image data from the coordinates of the extracted impulse signal. The digital watermark extraction module 103-3 detects in advance which frequency component of an image to be detected before scaling contains an impulse signal.

[0125]   The digital watermark extraction module 103-3 can calculate the scaling factor from the ratio of the frequency detected in advance to the frequency at which the impulse is detected. Letting a be the frequency detected in advance, and b be the frequency at which the impulse is detected, scaling at a/b is performed. This is the property of known Fourier transformation.

[0126]   The digital watermark extraction module 103-3 determines the size of a pattern for detecting a digital watermark contained in digital image data, and performs convolution using the pattern to detect the digital watermark contained in the digital image data.

[0127]   Note that the digital watermark may be added to any component constituting digital image data. In general, however, the digital watermark is added to a blue component to which the human visual sense is most insensitive. In this case, the above-described pattern detection is done for a blue component.

[0128]   When a digital watermark is not added to a visible color component constituting digital image data, but a digital watermark for embedding information in a specific frequency component is embedded in digital image data, processing may be done to detect the digital watermark for the specific frequency after the digital image data undergoes Fourier transformation.

[0129]   The digital watermark may be one which is embedded in a specific frequency in an image and c-annot be recognized with a naked eye, or one which is embedded in an image with an unnoticeable size and color and can be visually recognized. The digital watermark is preferably embedded in the pattern of an image because the digital watermark cannot be visually recognized.

[0130]   The digital watermark may contain, as code information, information about the type of image, the issue country, the issue number, and the value. This information may also be determined by the digital watermark

extraction module, and stored as log information as shown in Fig. 7. If the log information is stored in the folder of the HDD 108 by encrypting this information so as not to decrypt it without using a dedicated application, the log of processing the digital watermark-embedded image can be stored with high security.

[0131]   When the digital watermark-embedded image is processed by the digital watermark extraction module, the log information shown in Fig. 7 may be added as a digital watermark to a processed image. With this processing, even if an image is formed using a printer driver having no digital watermark extraction module, the added digital watermark can be detected from the print by the scanner driver.

[0132]   The fourth embodiment has described the digital watermark extraction module 103-3 as a software module. However, the digital watermark extraction module 103-3 can be realized by performing processing by hardware constituted by, e.g., a high-speed RISC and ASIC to increase the speed.

[0133]   After the image data is read and subjected to digital watermark extraction processing, the scanner driver 103 notifies in step S424 the OS 102 of the end of read processing, and at the same time returns the result representing whether information can be extracted, and extracted information.

[0134]   If the OS 102 receives the processing end notification from the scanner driver 103 in step S412, the OS 102 checks in step S413 whether a digital watermark is extracted. If the digital watermark is extracted, the OS 102 advances to step S414, and shifts to image processing (to be described in detail later).

[0135]   If the digital watermark is not extracted in step S413, and image processing ends, the OS 102 issues a processing end notification to the application 101. When the application 101 receives the processing end notification in step S403, image read operation of the scanner system ends.

[0136]   Details of image processing control processing (S414 shown in Fig. 16) performed by the image processing control module 116 will be described.

[0137]   Fig. 17 is a view showing an example of a user interface window displayed on the monitor 109. This example shows a window displayed to the user when digital watermark information is recognized to exist in image data read by the scanner 104.

[0138]   In Fig. 17, reference numeral 401 denotes a button which is selected and clicked by the user when the user approves the contents of a display and outputs extracted information by overlaying it on an image. Figs. 18A and 18B show an example of the image output at this time. Fig. 18A is an original image read by the scanner 104, and Fig. 18B is a result of overlaying extracted information on Fig. 18A.

[0139]   Reference numeral 402 in Fig. 17 denote a button which is selected by the user when the user approves the contents of a display and does not overlay the extracted information on the image output.

[0140]   Fig. 19 is a view showing an example of log information stored in the hard disk 108. This example shows information extracted from a digital watermark.

[Fifth Embodiment]

[0141]   The fourth embodiment has described a case wherein a digital watermark is extracted from an input image to execute predetermined image processing in a scanner system. The same processing can also be performed in a printer system. A system in the fifth embodiment will be explained.

[0142]   The arrangement of the system in the fifth embodiment is the same as that shown in Fig. 1, and a description thereof will be omitted.

[0143]   Fig. 20 is a block diagram showing the arrangement of an image processing apparatus in the fifth embodiment. According to the fifth embodiment, image processing is done by a printer driver 703 and OS 702 in the image processing system built by a host computer 21 and printer. Similar to the fourth embodiment, the OS 702 runs on the host computer 21, and an application 701 running on the OS 702 provides a manipulation environment for image output operation to a printer 704.

[0144]   Similar to the scanner system shown in Fig. 15, the printer system shown in Fig. 20 is also implemented on a hardware arrangement shown in Fig. 1. This system is built by the host computer 21 and printer 704. Both the OS 702 and application 701 on the host computer 21 realize image processing in the information processing apparatus by running by a CPU 204 a program loaded from an HDD 108 to a RAM 205.

[0145]   As shown in Fig. 20, the OS 702 has the printer driver 703 as a module for controlling a user input and another hardware device, and in addition controlling the printer 704. The printer driver 703 in the fifth-embodiment comprises a rasterizer 703-1 for generating image data suitable for the printer 704, a memory management module 703-2 for managing an image memory 710 for storing the generated image data, and a digital watermark extraction module 703-4 for extracting and processing information by a digital watermark in the rasterized image data.

[0146]   The OS 702 comprises an image processing control module 715 for executing image processing control processing (to be described in detail later) for an extraction result from the digital watermark extraction module 703-4, and a display driver 707 for displaying an output document, user interface window, and the like on a monitor 708. The extraction result as an output from the digital watermark extraction module 703-4 is transferred to the image processing control module 715, which performs processing of an image in accordance with the extraction result.

[0147]   The OS 702 has a printing spooler (spooler) 709 for performing control for outputting a rasterized image to the printer 704.

[0148]   Note that the rasterizer 703-1, image memory 710, and digital watermark extraction module 703-4 are adopted as the printer driver 703 and operated by software processing, but may be operated on the printer 704 side. In this case, the result of digital watermark extraction done by the printer 704 is returned to the image processing control module 715.

[0149]   An operation of extracting information embedded by a digital watermark in image data to be output from the host computer 21 to the printer 704, and executing image processing control processing will be described.

[0150]   Fig. 21 is a flow chart showing the processing sequence of the system in the fifth embodiment. This processing corresponds to data processing between the modules of the application 701, OS 102, and printer driver 703 shown in Fig. 20. S801 and S802 shown in Fig. 21 correspond to the steps of the application 701; S811 to S815, to the steps of the operating system 702; and S821 to S824, to the steps of the printer driver 703.

[0151]   When the user designates a desired document and printer via the application 701 and instructs the start of printing processing, a printing instruction command is sent to the OS 702. Then, the application 701 enters a wait state and stays there until the application 701 receives a printing processing end notification in step S802.

[0152]   In step S811, the OS 102 which has received the printing instruction command requests printing processing of a document received from the application 701, of the printer driver 703 corresponding to the designated printer (in the fifth embodiment, the printer 704), and enters a wait state and stays there until processing of the printer driver 703 ends. At this time, the OS 702 prepares a variable for information extracted from a digital watermark in image data output from the digital watermark extraction module 703-4.

[0153]   The rasterizer 703-1 in the printer driver 703 which has received the printing processing request from the OS 702 rasterizes a printing document as image data, and stores the image data in the image memory 710. In step S822, the digital watermark extraction module 703-4 extracts information embedded by a digital watermark from the image data stored in the image memory 710.

[0154]   At the same time when the image data is transferred to the digital watermark extraction module 703-4, it is also transferred to the spooler 709, and the printer 704 starts printing processing in step S823.

[0155]   After extraction and printing processing of information embedded by the digital watermark in the image data end, the printer driver 703 notifies the OS 702 of the end of printing processing in step S824, and at the same time returns the digital watermark extraction result and extracted information.

[0156]   The OS 702 receives the processing end notification of the printer driver 703 in step S812, and checks in step S813 whether a digital watermark is extracted. If the digital watermark is extracted, the OS 702 shifts

23   **EP 1 102 466 A2**   24

to image processing in step S814, and executes the same processing as that in the fourth embodiment.

[0157] After this processing ends, the OS 702 outputs a processing end notification to the application 701. If the application 701 receives the processing end notification in step S802, printing processing of this system ends.

[0158] The configuration of a data processing program readable by the information processing apparatus according to the present invention will be explained with reference to a memory map shown in Fig. 22.

[0159] Fig. 22 is a view for explaining a memory map to a storage medium which stores various data processing programs readable by the information processing apparatus according to the present invention.

[0160] Although not shown, this storage medium may store information for managing modules stored in the storage medium, such as version information and programmer name, and information depending on the OS of the program reading side, such as an icon for discriminatively displaying a program.

[0161] Further, data subordinate to various programs are also managed by directory information. In some cases, the storage medium also stores a program for installing various programs in a computer, or a program for decompressing a program to be installed when the program is compressed.

[0162] The functions shown in Figs. 16 and 21 may be achieved by the host computer in accordance with an externally installed program. The present invention is also applied to a case wherein pieces of information including a program is supplied to an output apparatus from a storage medium such as a CD-ROM, flash memory, or FD, or from an external storage medium via a network.

[0163] The objects of the present invention are also achieved by supplying a storage medium which records a program code of software that implements the functions of the above embodiments to a system or apparatus, and reading out and executing the program code stored in the storage medium by the computer (CPU or MPU) of the system or apparatus.

[0164] In this case, the program code read out from the storage medium implements the functions of the above embodiments, and the storage medium which stores the program code constitutes the present invention.

[0165] As the storage medium for supplying the program code, for example, a floppy disk, hard disk, optical disk, magneto-optical disk, CD-ROM, CD-R, magnetic tape, nonvolatile memory card, ROM, and the like can be used.

[0166] The functions of the above embodiments may be implemented not only by executing the readout program code by the computer but also by performing some or all of actual processes by an OS (Operating System) running on the computer on the basis of an instruction of the program code.

[0167] Furthermore, the present invention also includes a case wherein the program code read out from the storage medium is written in the memory of a function expansion board inserted into the computer or a function expansion unit connected to the computer, the CPU or the like of the function expansion board or function expansion unit performs some or all of actual processes in accordance with the instruction of the program code, and the functions of the above embodiments are realized by this processing.

[0168] As has been described above, according to these embodiments, embedded information can be output as visible information by extracting the information embedded in the image, processing the extracted information into an image, and outputting the image.

[0169] As many apparently widely different embodiments of the present invention can be made without departing from the spirit and scope thereof, it is to be understood that the invention is not limited to the specific embodiments thereof except as defined in the appended claims.

Claims

1. An information processing apparatus capable of controlling read operation of an original image by a scanner via a scanner driver, characterized by comprising:

   determination means (103-2) for determining . by the scanner driver whether digital watermark information is embedded in image data read by the scanner; and
   control means (106) for controlling predetermined image processing for the read image data on the basis of a determination result by said determination means.

2. The apparatus according to claim 1, wherein said control means processes the read image data into image data different from the read image data when said determination means determines that the read image data substantially matches the specific image data.

3. The apparatus according to claim 1, further comprising display means (109) for displaying a warning message representing that the image data is processed to match the specific image data when the predetermined image processing is performed for the read image data,
   wherein said control means discards the read and processed image data on the basis of an image processing request from a user in response to the warning message displayed on said display means.

4. The apparatus according to claim 3, wherein said

control means creates log information from which a read processing status of the specific image data can be verified, and registers the log information in a nonvolatile memory on the basis of the image processing request from the user in response to the warning message displayed on said display means.

5. The apparatus according to claim 1, wherein the predetermined image processing includes resolution conversion processing of converting a resolution of the read image data, color conversion processing of converting color tone of the read image data, and image conversion processing of adding arbitrary image data to the read image data.

6. The apparatus according to claim 1, wherein the specific image data is data of an original image whose copying operation is prohibited by law.

7. The apparatus according to claim 1, wherein the specific image data is stored and managed in advance so as to be updateable.

8. The apparatus according to claim 1, wherein the scanner can be connected via a local interface or a network interface.

9. The apparatus according to claim 1, wherein the digital watermark information is embedded in the specific image data at a predetermined cycle.

10. The apparatus according to claim 1, wherein the digital watermark information includes, as code information, information about the type of specific image data, an issue country, an issue number, and a value.

11. The apparatus according to claim 1, wherein the digital watermark information includes invisible or visible information.

12. The apparatus according to claim 1, further comprising storage means (110) for storing image data read by the scanner,
    wherein said control means also processes an image stored in said storage means.

13. An image processing method for an information processing apparatus capable of controlling read operation of an original image by a scanner via a scanner driver, characterized by comprising:

    a determination step (S323) of determining by the scanner driver whether digital watermark information is embedded in image data read by the scanner; and
    a control step (S314) of controlling predetermined image processing for the read image da-

ta on the basis of a determination result in the determination step.

14. The method according to claim 13, wherein the control step comprises processing the read image data into image data different from the read image data when the image data is determined in the determination step to substantially match the specific image data.

15. The method according to claim 13, further comprising a display step (S602) of displaying a warning message representing that the image data is processed to match the specific image data when the predetermined image processing is performed for the image data in the control step,
    wherein the control step comprises discarding the read and processed image data on the basis of an image processing request from a user in response to the warning message displayed in the display step.

16. The method according to claim 13, wherein the predetermined image processing includes resolution conversion processing of converting a resolution of the read image data, color conversion processing of converting color tone of the read image data, and image conversion processing of adding arbitrary image data to the read image data.

17. The method according to claim 13, wherein the control step comprises creating log information from which a read processing status of the specific image data can be verified, and registering the log information in a nonvolatile memory on the basis of the image processing request from the user in response to the warning message displayed in the display step.

18. The method according to claim 13, wherein the specific image data is data of an original image whose copying operation is prohibited by law.

19. The method according to claim 13, wherein the specific image data is stored and managed in advance so as to be updateable.

20. A computer-readable storage medium which stores a program for causing an information processing apparatus capable of controlling read operation of an original image by a scanner via a scanner driver, to execute

    a determination step of determining by the scanner driver whether digital watermark information is embedded in image data read by the scanner, and
    a control step of controlling predetermined im-

27   **EP 1 102 466 A2**   28

age processing for the read image data on the basis of a determination result in the determination step.

21. The medium according to claim 20, wherein the control step comprises processing the read image data into image data different from the read image data when the image data is determined in the determination step to substantially match the specific image data.

22. The medium according to claim 20, wherein

   the computer-readable storage medium records a program for causing the information processing apparatus to execute the display step of displaying a warning message representing that the image data is processed to match the specific image data when the predetermined image processing is performed for the image data in the control step, and
   the control step comprises discarding the read and processed image data on the basis of an image processing request from a user in response to the warning message displayed in the display step.

23. The medium according to claim 22, wherein the control step comprises creating log information from which a read processing status of the specific image data can be verified, and registering the log information in a nonvolatile memory on the basis of the image processing request from the user with respect to the warning message displayed in the display step.

24. The medium according to claim 20, wherein the predetermined image processing includes resolution conversion processing of converting a resolution of the read image data, color conversion processing of converting color tone of the read image data, and image conversion processing of adding arbitrary image data to the read image data.

25. An information processing apparatus capable of controlling read operation of an original image by a scanner via a scanner driver, characterized by comprising:

   information extraction means (103-3) for extracting, by the scanner driver, digital watermark information embedded in image data read by the scanner; and
   image processing means (116) for processing the image data on the basis of an extraction result from said information extraction means.

26. The apparatus according to claim 25, further com-

prising selection means (109) for causing a user to select whether to process the image data by said image processing means.

27. The apparatus according to claim 26, wherein said selection means displays whether to process the image data on display means, thereby causing the user to select whether to process the image data.

28. The apparatus according to claim 25, wherein said image processing means overlays the information extracted by said information extraction means on the image data.

29. A processing method for an information processing apparatus capable of controlling read operation of an original image by a scanner via a scanner driver, characterized by comprising:

   an information extraction step (S423) of extracting, by the scanner driver, digital watermark information embedded in image data read by the scanner; and
   an image processing step (S413) of processing the image data on the basis of an extraction result in the information extraction step.

30. A computer-readable storage medium which stores a program for causing an information processing apparatus capable of controlling read operation of an original image by a scanner via a scanner driver, to execute

   an information extraction step of extracting, by the scanner driver, digital watermark information embedded in image data read by the scanner; and
   an image processing step of processing the input image data on the basis of an extraction result.

31. A method of performing processing in an operating system and a scanner driver to control an image read operation by a scanner to prevent the generation of image data faithfully representing a copy-prohibited image, comprising:

   determining whether image data representing an image read by the scanner has predetermined characteristics indicating that the image is copy-prohibited; and
   processing the image data if it is determined that the image is copy-prohibited so that the image data does not faithfully represent the image.

32. An operating system for a computer processing apparatus having processor-implementable instruc-

29   **EP 1 102 466 A2**   30

tions for causing the apparatus to perform at least one on the processing operations of:

> determining whether image data representing an image read by a scanner has predetermined characteristics indicating that the image is copy-prohibited; and
> processing image data representing an image read by the scanner if instructions are received indicating that the image is copy-prohibited so that the image data does not faithfully represent the image.

33. A printer driver for a computer processing apparatus comprising at least one of:

> means for determining whether image data representing an image read by a scanner has predetermined characteristics indicating that the image is copy-prohibited; and
> means for processing image data representing an image read by the scanner if instructions are received indicating that the image is copy-prohibited so that the image data does not faithfully represent the image.

34. A signal conveying instructions for causing a programmable processing apparatus to become operable to perform processing to carry out a method as set out in at least one of claims 13 to 19, 29 and 31.
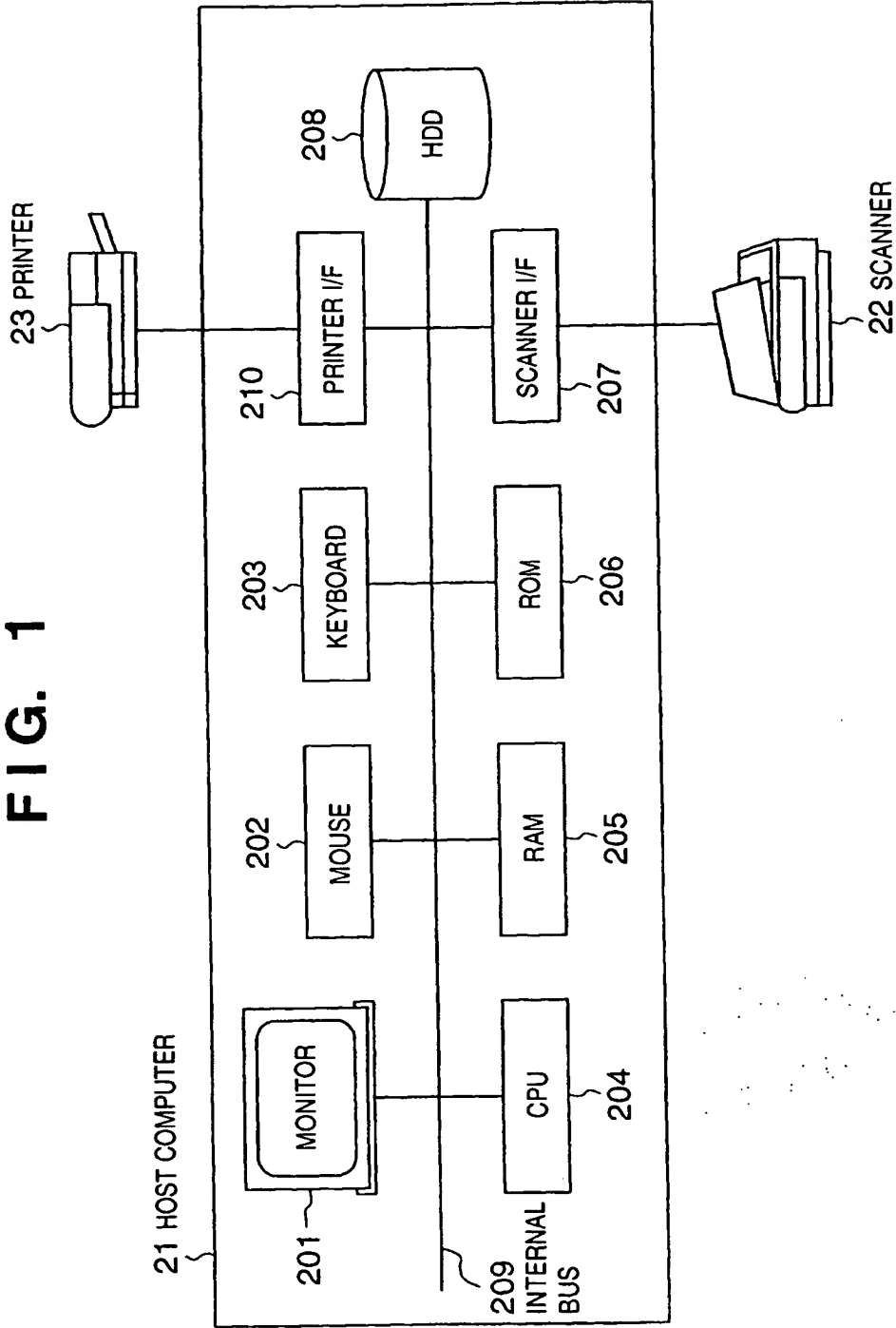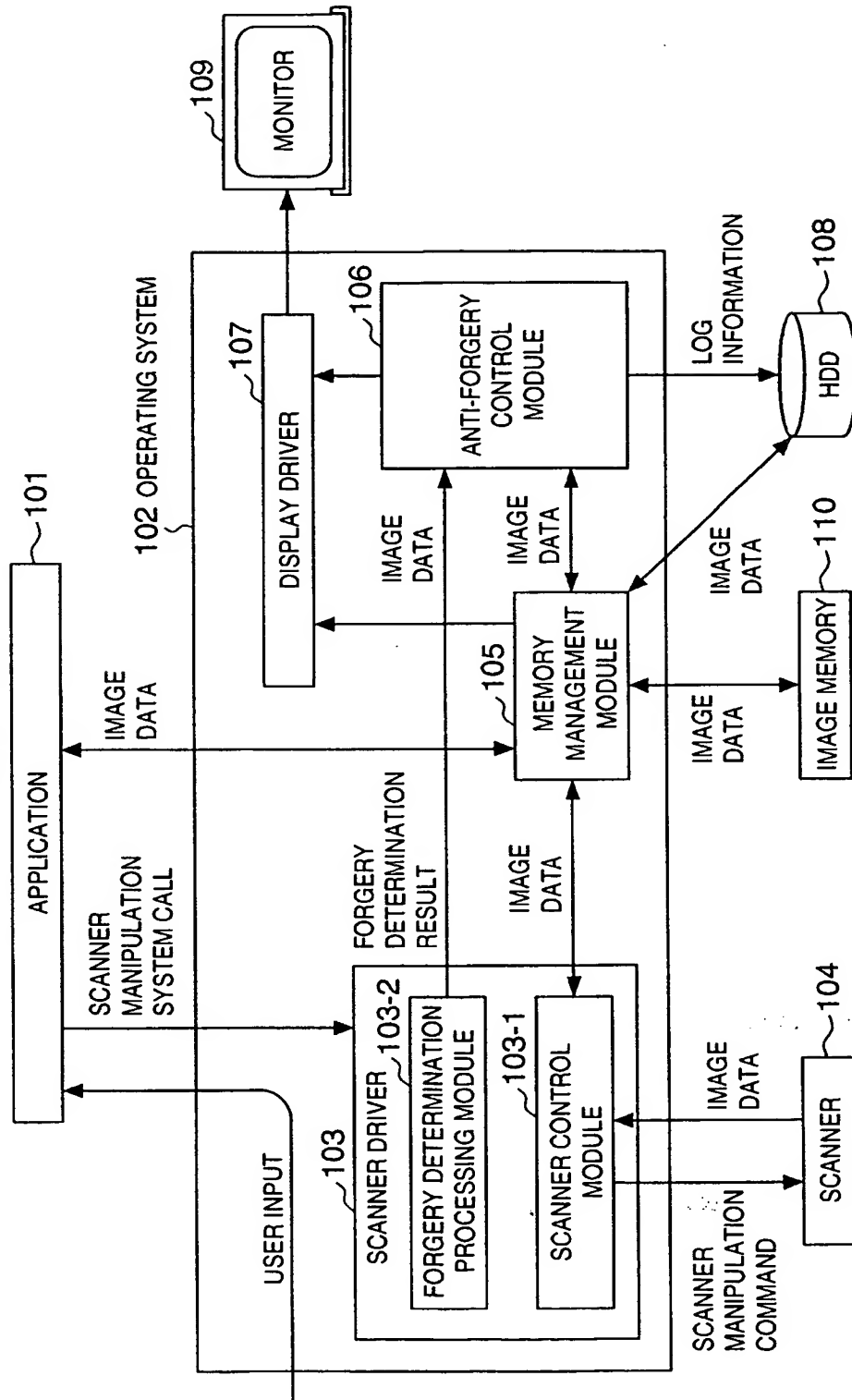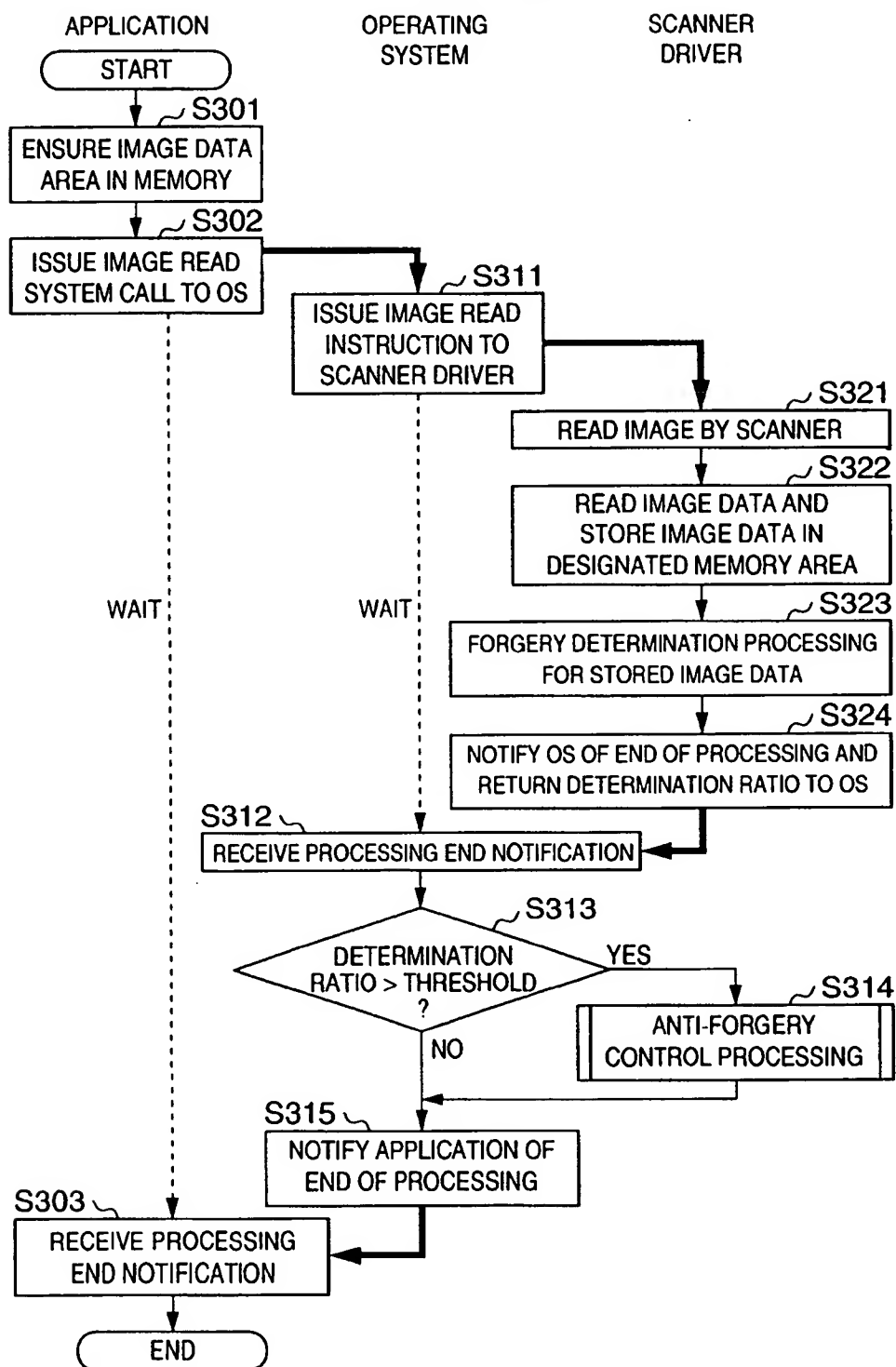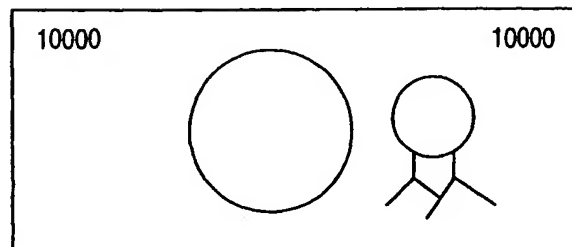
EP 1 102 466 A2

F I G. 1

21 HOST COMPUTER

23 PRINTER

22 SCANNER

MONITOR
201

MOUSE
202

KEYBOARD
203

PRINTER I/F
210

208
HDD

CPU
204

RAM
205

ROM
206

SCANNER I/F
207

209 INTERNAL BUS

FIG. 2

FIG. 3

APPLICATION

OPERATING SYSTEM

SCANNER DRIVER

START

S301 — ENSURE IMAGE DATA AREA IN MEMORY

S302 — ISSUE IMAGE READ SYSTEM CALL TO OS

S311 — ISSUE IMAGE READ INSTRUCTION TO SCANNER DRIVER

S321 — READ IMAGE BY SCANNER

S322 — READ IMAGE DATA AND STORE IMAGE DATA IN DESIGNATED MEMORY AREA

S323 — FORGERY DETERMINATION PROCESSING FOR STORED IMAGE DATA

S324 — NOTIFY OS OF END OF PROCESSING AND RETURN DETERMINATION RATIO TO OS

WAIT

WAIT

S312 — RECEIVE PROCESSING END NOTIFICATION

S313 — DETERMINATION RATIO > THRESHOLD ?

YES

S314 — ANTI-FORGERY CONTROL PROCESSING

NO

S315 — NOTIFY APPLICATION OF END OF PROCESSING

S303 — RECEIVE PROCESSING END NOTIFICATION

END

EP 1 102 466 A2

F I G. 4A

ORIGINAL IMAGE

F I G. 4B
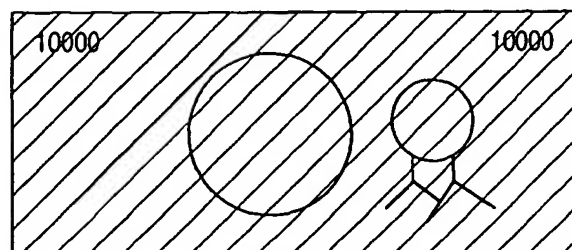
PROCESSED IMAGE

EP 1 102 466 A2

FIG. 5

ORIGINAL IMAGE

PROCESSED IMAGE

SCANNING POSITION

IMAGE DATA (GREEN)

255

0

I

II

EP 1 102 466 A2

F I G. 6

WARNING : This image is an image whose
copying operation is prohibited
by law.

Do you really process this image ?
(Note that this image has already been
processed.)

OK   Cancel

BT1   BT2
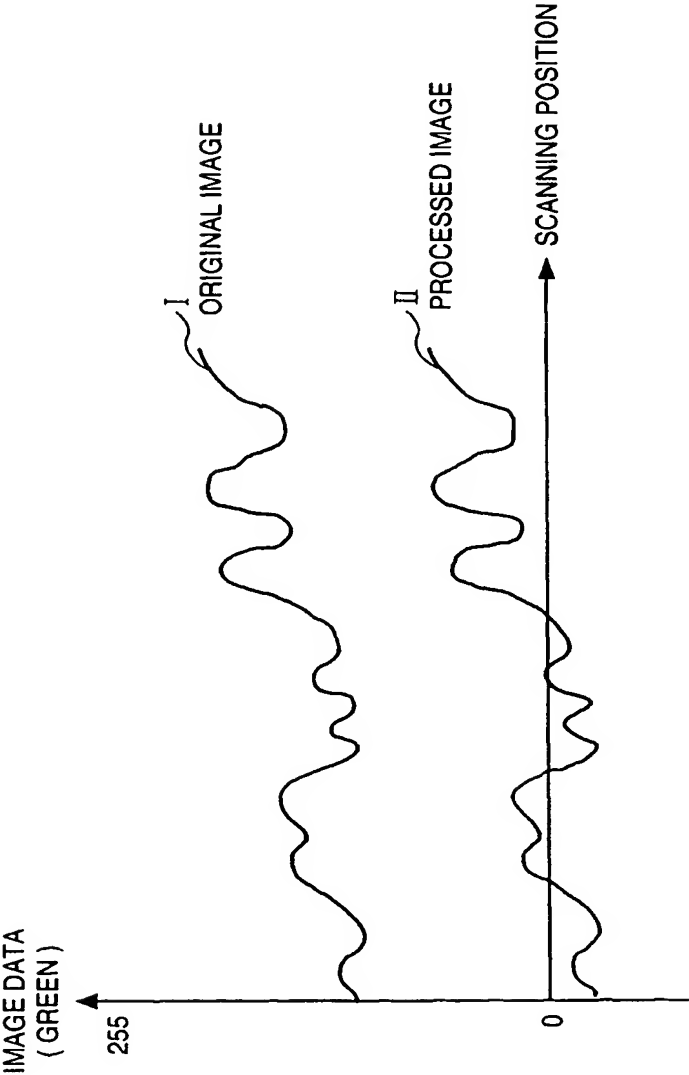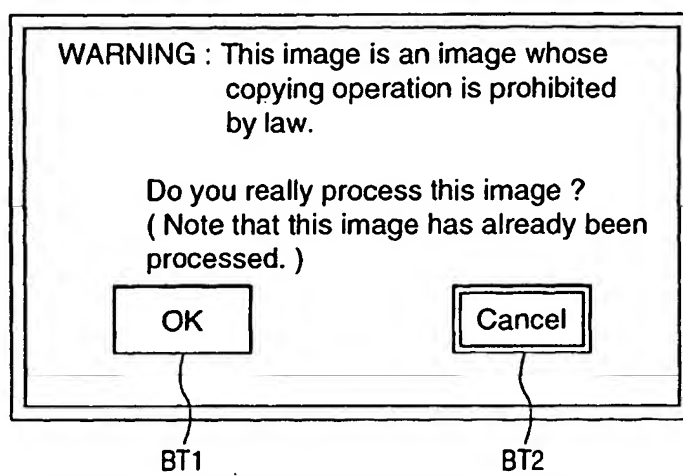
EP 1 102 466 A2

F I G. 7

LOG INFORMATION

TIME :	1999/11/15/10 : 00
HOST COMPUTER INFORMATION :	
· MANUFACTURER NAME	
· HOST ID	
· OS VERSION	
IMAGE SIZE :	2500x800
DETERMINATION RATIO :	95%

EP 1 102 466 A2

FIG. 8

```
        ┌─────────────┐
        │    START    │──S600
        └──────┬──────┘
               ▼
 ┌──────────────────────────┐
 │  PROCESS IMAGE IN MEMORY │──S601
 └────────────┬─────────────┘
              ▼
 ┌──────────────────────────┐
 │  DISPLAY WARNING DIALOG   │──S602
 └────────────┬─────────────┘
              ▼          S603
          ◇─────────────◇    NO
         ╱  INPUT        ╲─────────┐          S604
        ◇   MESSAGE ?     ◇        ▼   ┌──────────────────┐
         ╲               ╱   ┌──────────│ FREE IMAGE MEMORY │
          ◇─────────────◇    │     └──────────────────┘
              │YES           │
              ▼              │
        ┌─────────────┐◄─────┘
        │     END     │──S605
        └─────────────┘
```

EP 1 102 466 A2

FIG. 9

F I G. 10
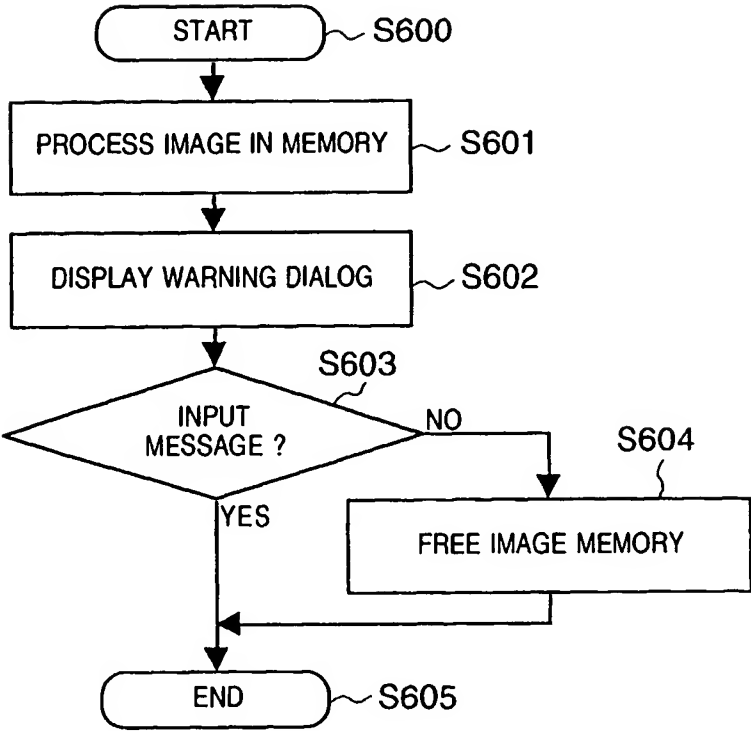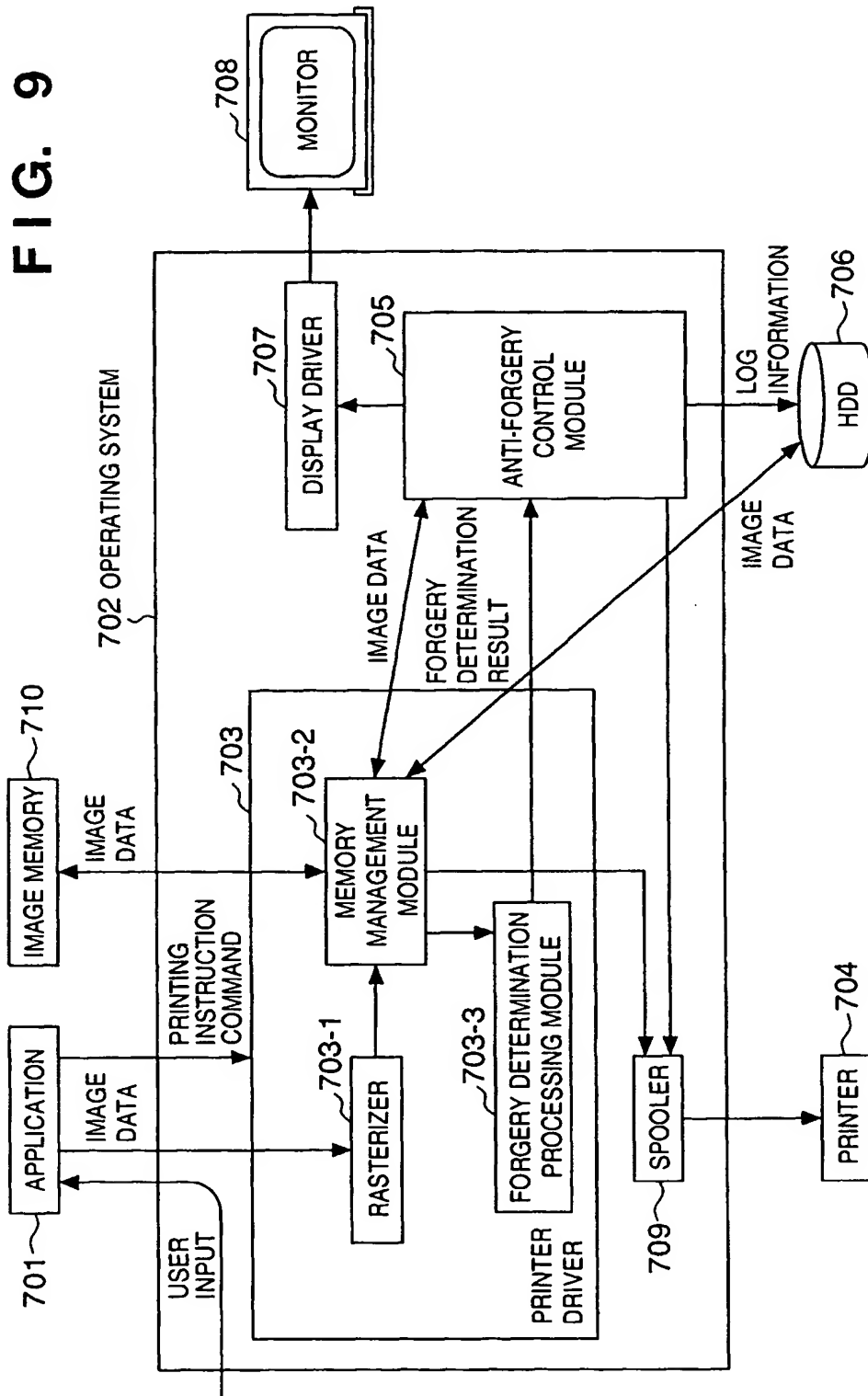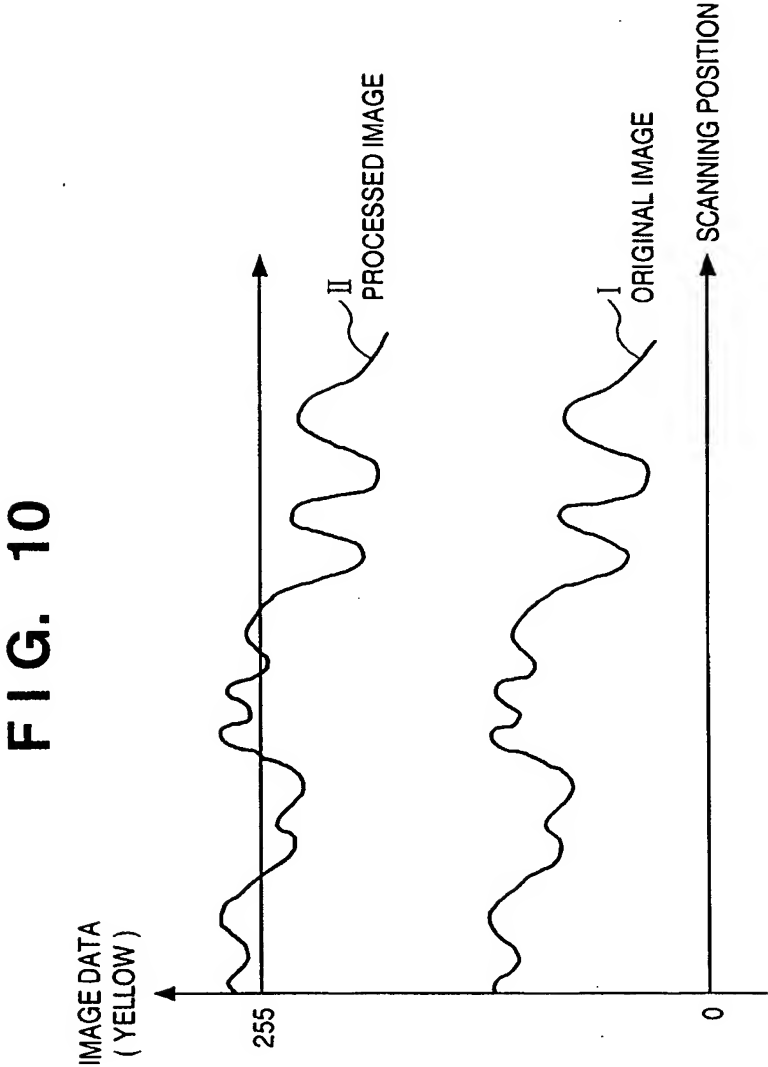
EP 1 102 466 A2

FIG. 11

FIG. 12

12-1

12-2
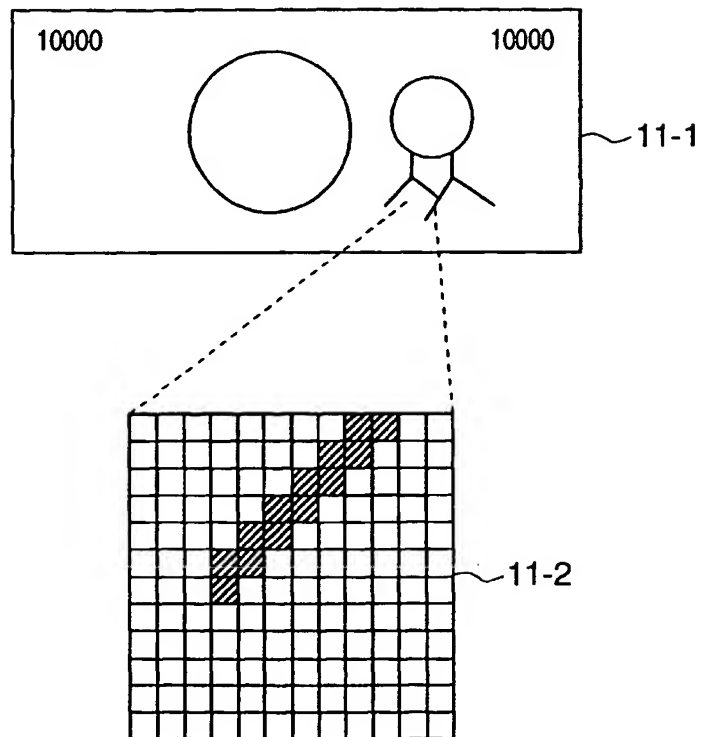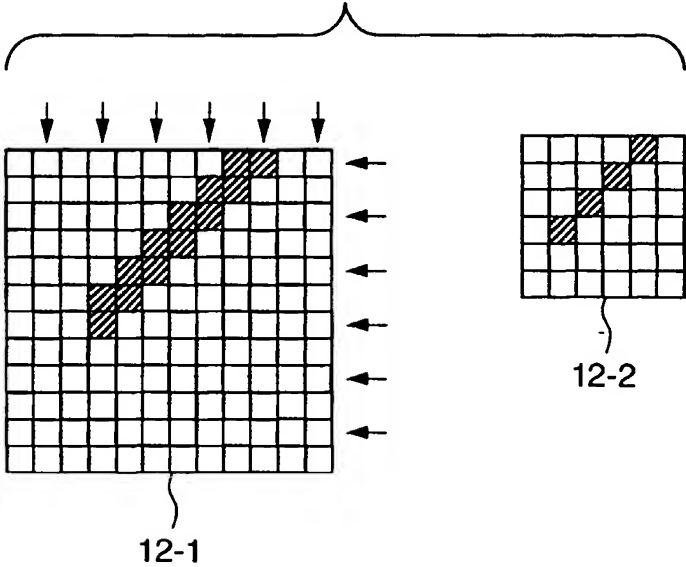
EP 1 102 466 A2

F I G. 13

10000   10000

COPY
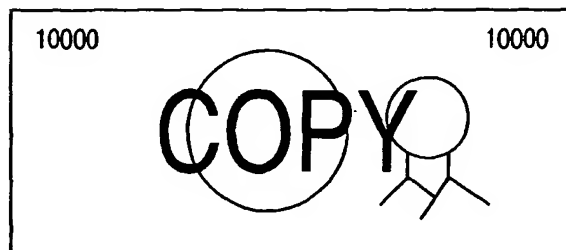
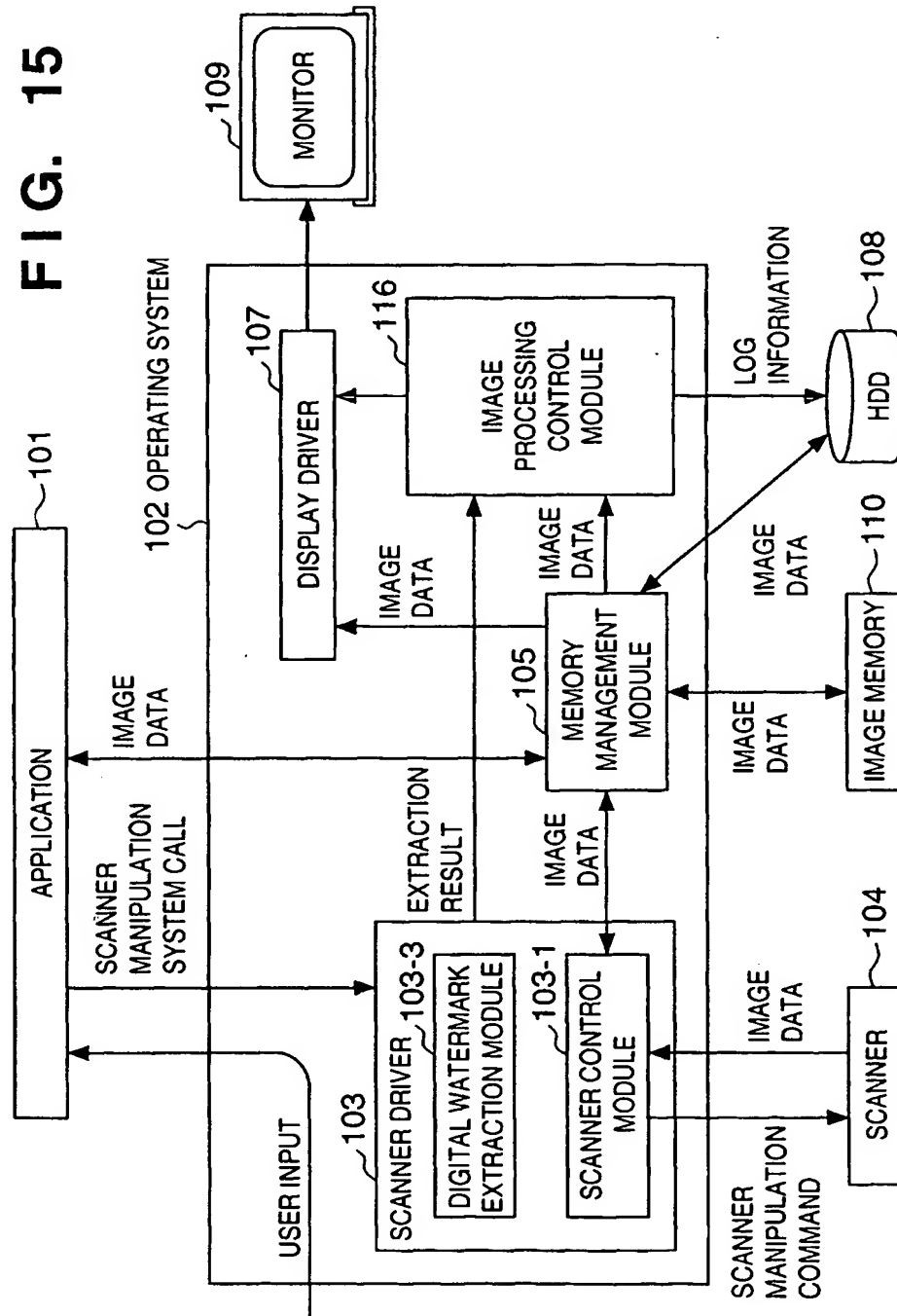**EP 1 102 466 A2**

FIG. 14

STORAGE MEDIUM SUCH AS FD/CD-ROM

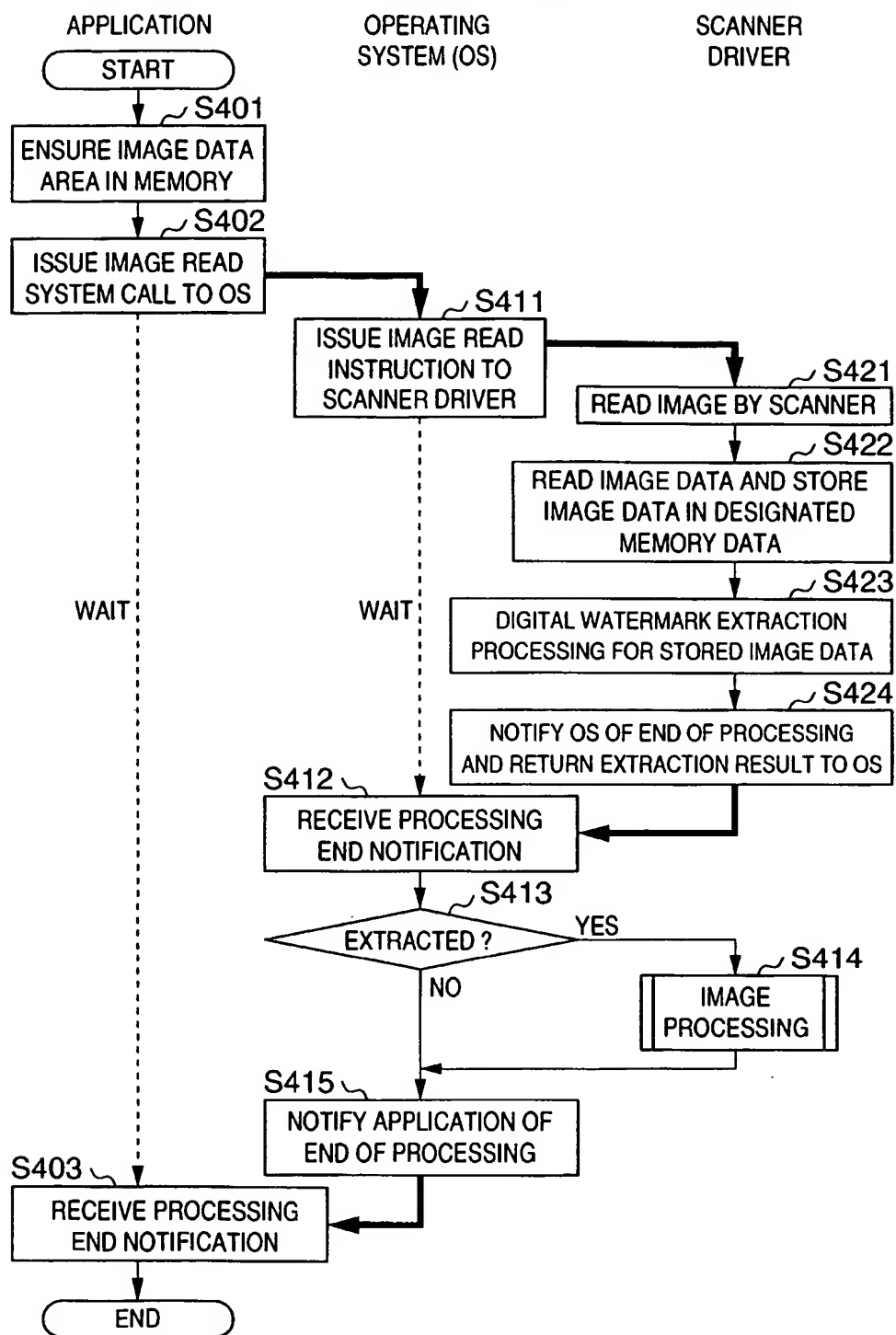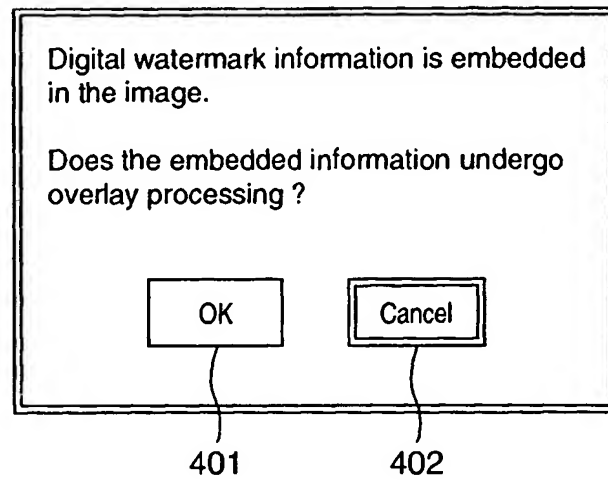| DIRECTORY INFORMATION |
|---|
| FIRST DATA PROCESSING PROGRAM
PROGRAM CODES CORRESPONDING TO STEPS OF
FLOW CHART SHOWN IN FIG. 3 |
| SECOND DATA PROCESSING PROGRAM
PROGRAM CODES CORRESPONDING TO STEPS OF
FLOW CHART SHOWN IN FIG. 8 |
| |

MEMORY MAP OF STORAGE MEDIUM
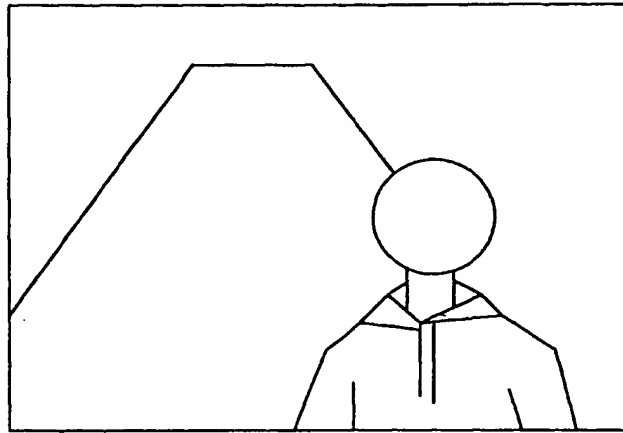
EP 1 102 466 A2

F I G. 15

EP 1 102 466 A2

F I G.   16

APPLICATION   OPERATING   SCANNER
                           SYSTEM (OS)   DRIVER

(START)

↓ S401

ENSURE IMAGE DATA
AREA IN MEMORY

↓ S402

ISSUE IMAGE READ
SYSTEM CALL TO OS

S411

ISSUE IMAGE READ
INSTRUCTION TO
SCANNER DRIVER

S421

READ IMAGE BY SCANNER

↓ S422

READ IMAGE DATA AND STORE
IMAGE DATA IN DESIGNATED
MEMORY DATA

↓ S423

DIGITAL WATERMARK EXTRACTION
PROCESSING FOR STORED IMAGE DATA

↓ S424

NOTIFY OS OF END OF PROCESSING
AND RETURN EXTRACTION RESULT TO OS

WAIT   WAIT

S412

RECEIVE PROCESSING
END NOTIFICATION

↓ S413

EXTRACTED ?   YES   S414

NO   IMAGE
                                PROCESSING

S415

NOTIFY APPLICATION OF
END OF PROCESSING

S403

RECEIVE PROCESSING
END NOTIFICATION

↓

(END)

EP 1 102 466 A2

FIG. 17

Digital watermark information is embedded in the image.

Does the embedded information undergo overlay processing ?

| OK | | Cancel |

401   402

EP 1 102 466 A2

F I G. 18A

F I G. 18B

2001.02.01
AT Mt. FUJI

EP 1 102 466 A2

F I G. 19

DIGITAL WATERMARK
EXTRACTION RESULT

2001.02.01
AT Mt. FUJI

F I G. 20

F I G. 21

APPLICATION

OPERATING
SYSTEM (OS)

PRINTER
DRIVER

START

S801

SEND PRINTING
INSTRUCTION
COMMAND TO OS

S811

REQUEST PRINTING
PROCESSING OF
PRINTER DRIVER

S821

RASTERIZE PRINTING DOCUMENT
TO IMAGE DATA AND STORE IMAGE
DATA IN IMAGE MEMORY

S822

EXTRACT DIGITAL WATERMARK
FROM STORED IMAGE DATA

S823

PRINTING PROCESSING

S824

NOTIFY OS OF END OF
PROCESSING AND RETURN
EXTRACTION RESULT TO OS

S812

RECEIVE PROCESSING END
NOTIFICATION

S813

EXTRACTED ?

YES

S814

IMAGE
PROCESSING

NO

S815

NOTIFY APPLICATION OF
END OF PROCESSING

S802

RECEIVE PROCESSING
END NOTIFICATION

END

EP 1 102 466 A2

F I G.   22

STORAGE MEDIUM SUCH AS FD/CD-ROM

DIRECTORY INFORMATION
FIRST DATA PROCESSING PROGRAM PROGRAM CODES CORRESPONDING TO STEPS OF FLOW CHART SHOWN IN FIG. 16

MEMORY MAP OF STORAGE MEDIUM